April 24, 2021 16:31 MYT
KUALA LUMPUR: Kes-kes penipuan 'memancing data' perbankan internet dilihat semakin meningkat sejak kebelakangan ini. Pelbagai taktik digunakan termasuk menerusi panggilan telefon, menghantar khidmat pesanan ringkas (SMS) secara rambang menyerupai pesanan bank dan juga kiriman emel bagi memperdaya pengguna supaya menyerahkan maklumat peribadi seperti nama dan kata laluan akaun perbankan Internet. Baru-baru ini Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) mendedahkan beberapa helah dan modus operandi yang digunakan scammer itu. Modus operandi itu turut digunakan untuk memperdaya dan memperoleh nombor Transaction Authorization Code (TAC) atau One-Time PIN (OTP) daripada pengguna. Berikut modus operandi yang dikesan digunakan scammer: 1. Pesanan ringkas SMS atau mana-mana aplikasi pesanan termasuk WhatsApp dihantar menyatakan berlakunya transaksi kewangan mencurigakan atau wujud keperluan untuk pengguna mengesahkan, mengemas kini atau mengaktifkan semula akaun perbankan Internet. 2. Pengguna diminta untuk melayari pautan laman sesawang palsu yang diberikan dan kemudian memasukkan nama dan kata laluan akaun perbankan Internet. 3. Paparan di laman sesawang palsu itu akan kelihatan serupa dengan laman sesawang perbankan Internet sebenar namun alamat URL laman itu mempunyai perbezaan dan variasi dari segi nama, huruf serta ejaan. 4. Modus operandi itu termasuk meminta pengguna menghubungi talian penting (hotline) palsu dan seterusnya pengguna akan berhubung dengan scammer yang menyamar sebagai pegawai bank atau pihak berkuasa. 5. Melalui interaksi itu, pengguna kemudian diminta melayari laman sesawang palsu dan perlu memasukkan nama pengguna serta kata laluan akaun perbankan internet atau diminta memuat turun dan memasang aplikasi palsu dalam bentuk fail 'APK', yang memerlukan mereka memasukkan nama pengguna dan kata laluan akaun perbankan Internet. &#65533; Sumber: https://www.astroawani.com/berita-malaysia/awas-jangan-terpedaya-scammer-pancing-data-294901